Riktlinje för informationssäkerhet och dataskydd

Dokumenttyp **Riktlinje**	*Diarienummer* **2025-86**
Beslutad av (dokumentägare) **Kommunstyrelsen**	*Beslutsdatum och ev. paragraf* **KS 2026-02-17, §7**
Dokumentansvarig **IT-chef**	*Senast reviderad (datum)* Klicka eller tryck här för att ange text.
Gäller för **Hofors kommun**	*Giltig t.o.m. (datum eller tillsvidare)* **Tillsvidare**

Innehållsförteckning

Inledning **1**
Syfte 1
Omfattning och avgränsningar 1
Om informationssäkerhet och dataskydd **1**
Informationssäkerhet som samlingsterm 1
Dataskyddsförordningen och andra bestämmelser om dataskydd 2
Cybersäkerhetslagen 2
Organisation för informationssäkerhetsarbete i Hofors kommun **3**
Specifika nyckelfunktioner 3
Ansvarsfördelning inom politik och förvaltning 4
Politiken 4
Kommunförvaltningen 4
Arbetssätt och skyddsåtgärder **5**
Ledningssystem för informationssäkerhet och dataskydd - LISD 5
Kontinuitetsplanering 5
Informationstillgångar, informationsklassning och konsekvensbedömning 5
Information om och hantering av registrerades rättigheter 6
Hantering av artificiell intelligens (AI) 6
Utbildning och avslut av anställning 7
Upphandling, kravspecifikation och uppföljning av externa parter 7
Upphandling och införande av IT-system 7
Externa parter 8
Nätverks- och systemsäkerhet 8
Driftsäkerhet 8
Nätverk 9
Enheter och applikationer 9
Fysisk och miljörelaterad säkerhet 10
Incidenthantering 10

Inledning

Ändamålsenlig informationssäkerhet och skydd för den personliga integriteten förutsätter ett strukturerat och systematiskt arbete som är integrerat i det dagliga arbetet i alla verksamheter som hanterar information. Genom ett samordnat arbete mellan verksamhet och andra stödfunktioner kan väl avvägda bedömningar för lämpliga säkerhetsåtgärder göras och en god och säker informationshantering uppnås.

Syfte

Denna riktlinje beskriver hur Hofors kommun ska bedriva ett systematiskt arbete inom informationssäkerhet och dataskydd som är ändamålsenligt, rättssäkert och effektivt samt håller god kvalitét. Riktlinjen kompletterar gällande bestämmelser i lag och förordning genom att konkretisera utvalda delar och tydliggöra hur reglerna ska tillämpas i kommunen. Riktlinjerna ska därför läsas tillsammans med dessa bestämmelser. Riktlinjen ska även tydliggöra ansvarsfördelningen i dessa frågor.

Omfattning och avgränsningar

Den här riktlinjen gäller i sin helhet för Hofors kommun. Riktlinjen kompletteras av rutiner och stödmaterial, såsom handböcker och mallar. Kraven på informationssäkerhet och dataskydd som ställs i denna riktlinje gäller även samtliga externa aktörer som på något vis har åtkomst till kommunens IT-miljö. Hur dessa väljer att organisera sig för att leva upp till kraven är upp till dem.

Denna riktlinje anger endast hur arbetet ska utföras i kommunen. Direktiv för verksamheternas implementering av riktlinjens krav fastslås av respektive nämnd i separata handlings- och åtgärdsplaner, i enlighet med kommunens riktlinje för styrdokument.

Om informationssäkerhet och dataskydd

Informationssäkerhet som samlingsterm

Informationssäkerhet handlar om att hantera alla former av informationstillgångar i en organisation så att i huvudsak tre kriterier säkerställs: informationens riktighet, tillgänglighet och konfidentialitet. Kortfattat innebär detta att informationen ska skyddas mot obehöriga, även internt, samtidigt som den är tillgänglig och oförvanskad när den behövs i organisationen. En annan viktig aspekt är att informationshanteringen ska vara spårbar i organisationen.

Infosäk handlar också om mycket mer än bara IT-system och datalagring. Det gäller alla former av informationstillgångar i en organisation, inklusive muntliga samtal mellan kollegor och handskrivna anteckningar etcetera. Denna bredd gör också ämnet komplext och många begrepp används i olika sammanhang så som IT-säkerhet, Cybersäkerhet, Dataskydd etcetera. Informationssäkerhet är samlingstermen för alla dessa och det finns olika lagar inom området. Just dataskydd är ett område med speciallagstiftning som ställer krav på hur organisationen ska arbeta med personuppgifter. I januari 2026 trädde även Cybersäkerhetslagen i kraft, som ställer

tydliga krav på systematiskt informationssäkerhetsarbete i organisationer som på något sätt arbetar med samhällsviktig verksamhet.

Dataskyddsförordningen och andra bestämmelser om dataskydd

Dataskyddsförordningen (EU 2016/679), även kallad GDPR (General Data Protection Regulation), gäller i hela EU och för alla myndigheter, företag och organisationer som behandlar personuppgifter. Grunden till dataskyddet hittas i Europakonventionen om de mänskliga rättigheterna samt i EU:s stadga om de grundläggande rättigheterna och handlar kort beskrivet om individens rätt till sitt privatliv.

Syftet med dataskyddsförordningen är att skydda individens grundläggande fri- och rättigheter. Samtidigt ska förordningen skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Förordningen behandlar bland annat:

- Vilka principer dataskyddsarbetet ska stödja sig på
- Vilka rättigheter den registrerade har
- Hur personuppgifter får användas och ska hanteras i olika sammanhang
- Hur ett strategiskt dataskyddsarbete ska gå till

Det finns flera andra bestämmelser som också reglerar på vilket sätt personuppgifter får och ska hanteras. Samtidigt ska de möjliggöra hantering av personuppgifter utifrån de samhällsbehov som finns. De olika bestämmelserna återfinns i bland annat i brottsdatalagen (2018:1177), dataskyddslagen (2018:218), skollagen (2010:800), socialtjänstlagen (2025:400) och AI-förordningen (EU 2024/1689). Därtill finns ett antal registerförfattningar som bland annat gäller kommunal verksamhet. Några exempel är patientdatalagen (2008:355), lag (2001:454) om behandling av personuppgifter inom socialtjänsten och kamerabevakningslagen (2018:1200).

Cybersäkerhetslagen

Syftet med Cybersäkerhetslagen är att skydda informationstillgångar inom samhällsviktig verksamhet. Verksamhetsutövare ska vidta ett antal säkerhetsåtgärder inom flera områden, exempelvis incidenthantering, säker och begränsad åtkomst till system och nätverk, kontinuitetshantering, upphandling samt utbildning och personalsäkerhet.

Organisation för informationssäkerhetsarbete i Hofors kommun

Specifika nyckelfunktioner

Nyckelfunktionerna nedan utgör den samlade expertisen inom infosäk och dataskydd. På många sätt står varje nyckelfunktion på egna ben i sina respektive ansvar. Ett välfungerande systematiskt arbete inom infosäk och dataskydd kräver dock även en gränsöverskridande samverkan mellan dessa funktioner, oavsett organisatorisk hemvist.

- *Informationssäkerhetssamordnare* – Leder, samordnar, utvecklar och följer upp det övergripande informationssäkerhetsarbetet, bland annat genom samordningen av LISD. Informationssäkerhetssamordnaren är också ett stöd till verksamheterna i det operativa arbetet som vid exempelvis informationsklassning och utbildningsinsatser.
- *Dataskyddsombud (DSO)* – Ger råd, stöd samt bevakar att personuppgiftsansvarig lever upp till dataskyddsförordningen och annan relevant lagstiftning. Dataskyddsombudet har inget ansvar för att dataskyddsförordningen följs. Det ansvaret ligger alltid hos den personuppgiftsansvariga. Varje styrelse och nämnd ska ha ett utsett dataskyddsombud.
- *Dataskyddssamordnare (DSS)* - Utgör kontaktperson gentemot DSO. Samordnar styrelsen/nämndens dataskyddsarbete samt är ett stöd till verksamheten/enheten i det operativa arbetet med dataskydd. Verkar för en kommungemensam tillämpning av interna styrdokument och att bestämmelser gällande dataskydd efterlevs. Dataskyddssamordnare är inte ansvarig för att verksamheten/enheten följer dataskyddsförordningen. Varje styrelse och nämnd ska ha en utsedd dataskyddssamordnare.
- *Kontaktperson för informationssäkerhet och dataskydd* - Medarbetare i linjeorganisationen som är en kontaktperson gentemot informationssäkerhetssamordnare och DSS i det operativa infosäk- och dataskyddsarbetet. Kontaktpersonerna ska ingå i ett nätverk.
- *Säkerhetsskyddschef* - Ansvarig för skyddet av säkerhetsskyddsklassificerad information, det vill säga information som, om den röjs, kan medföra skada på Sveriges säkerhet.
- *Signalskyddschef samt biträdande signalskyddschef* - Ansvariga för bland annat hanteringen av krypterad säkerhetsskyddsklassificerad information.
- *Systemägare* – Övergripande ansvarig chef för de system som förvaltas inom dennes verksamhet.
- *Systemförvaltare* – Operativt ansvarig för ett eller flera system som organisationen använder sig av. Förvaltaren leder och samordnar arbetet med systemet/systemen samt rapporterar arbetet till systemägaren. Systemförvaltaren utgör kontaktperson till IT-tekniker.

Ansvarsfördelning inom politik och förvaltning

Politiken

- *Kommunfullmäktige*, har ett övergripande ansvar för kommunens informationssäkerhetsarbete och sätter ramarna för nämndernas arbete genom att besluta om bland annat mål och budget.
- *Kommunstyrelsen och nämnder*, är ytterst ansvariga för att informationssäkerhetsarbetet utförs i enlighet med gällande lagstiftning och av fullmäktige fastställda styrdokument. Kommunstyrelsen samordnar det övergripande informationssäkerhetsarbetet för att upprätthålla en effektiv och ändamålsenlig organisation. Det är styrelsen och nämnderna som är personuppgiftsansvariga (PUA), vilket innebär att de ansvarar för att verksamheten lever upp till dataskyddsförordningen och övriga bestämmelser gällande dataskydd. Personuppgiftsansvaret kan inte delegeras.
- *Enskilda förtroendevalda* - Ansvarar för att skydda organisationens information, särskilt känsliga personuppgifter och sekretessuppgifter, från obehörig åtkomst, modifiering eller läckage. Det åligger varje enskild förtroendevald att säkerställa att organisationen följer gällande lagar, standarder och övrig styrning inom informationssäkerhet och dataskydd genom att följa upp arbetet systematiskt. Det är den förtroendevaldes ansvar att agera på ett sätt som bygger och bibehåller det förtroende som medborgarna har för den offentliga organisationen.

Kommunförvaltningen

Ansvaret för informationssäkerhet och dataskydd följer ordinarie verksamhetsansvar. Det ska alltid finnas en informationsägare – det vill säga en funktion/befattning som har ansvaret för den information som skapas och hanteras inom den egna organisationen. Informationsägarskapet sammanfaller med ansvaret i verksamheten. Detta gäller från kommunledning till enskild medarbetare och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten och dataskyddet inom det verksamhetsområdet. Informationsägarens ansvar beskrivs mer i detalj nedan.

- *Kommunchef, VD, Sektorschef, Verksamhets-, Funktions- samt Enhetschefer*
  - Ansvarar för att arbetet bedrivs enligt gällande lagar, standarder och övrig styrning inom informationssäkerhet och dataskydd. Chefen ska skapa förutsättningar för verksamhetens implementering och efterlevnad av dem. Frågorna ska ges utrymme i verksamhetens planering och ske (om inget annat anges) inom ramen för den budget som verksamheten tilldelats. Respektive chef ska också säkerställa att verksamheten har tillräckligt många kontaktpersoner för ett effektivt arbete med informationssäkerhet och dataskydd. Detta görs i samråd med informationssäkerhetssamordnare och DSS. Chefen ska även återrapportera verksamhetens infosäk- och dataskyddsarbete.

- *Medarbetare* - Ansvarar för att skydda organisationens information, särskilt känsliga personuppgifter och sekretessuppgifter, från obehörig åtkomst, modifiering eller läckage. Det åligger varje enskild medarbetare att följa gällande lagar, standarder och övrig styrning inom informationssäkerhet och dataskydd samt att agera på ett sätt som bygger och bibehåller det förtroende som medborgarna har för den offentliga organisationen. Detsamma gäller även för vikarier, praktikanter och inhyrd personal.

Arbetssätt och skyddsåtgärder

Att Hofors kommun arbetar förebyggande med informationssäkerhet och dataskydd är en förutsättning för att undvika att informationssäkerhets- eller personuppgiftsincidenter inträffar eller att någon inte får sina rättigheter tillgodosedda. Alla kommunens processer ska ha ett integritetsfokus från start till utveckling, användning och avveckling.

Ledningssystem för informationssäkerhet och dataskydd - LISD

För att få en överblick av det systematiska arbetet ska kommunen arbeta i ett ledningssystem för informationssäkerhet och dataskydd, kallat LISD. Syftet är att samla alla mål- och styrdokument, organisationsbeskrivningar och processer för informationssäkerhet, dataskydd, cybersäkerhet samt IT-säkerhet på samma plats.

Kontinuitetsplanering

Ytterligare en viktig del inom informationssäkerhet är att förbereda organisationen på att klara av olika former av störningar och avbrott i system och arbetsprocesser som drabbar informations- och personuppgiftshanteringen. För att uppnå detta ska alla informationsägande verksamheter och personuppgiftsansvariga nämnder genomföra en så kallad kontinuitetsplanering. Detta består i att ta fram lämpliga reserv-, återställnings- samt återgångsrutiner för kritiska system och processer. För mer information om detta, se *Riktlinje för kontinuitetsplanering*.

Informationstillgångar, informationsklassning och konsekvensbedömning

En informationstillgång innefattar både informationen i sig, bärare av information och de system som hanterar informationen. Det kan bland annat vara:

- Dokument (fysiska och digitala)
- Strukturerad data (data som lagras i databaser eller andra digitala format)
- IT system och applikationer (som används för att hantera och behandla information)
- Datorer och annan hårdvara (som används för att lagra och bearbeta information)

En informationsklassning genomförs för att bedöma skyddsbehovet för informationen och vid en konsekvensbedömning bedöms de eventuella konsekvenser som behandlingen kan medföra för de människor vars uppgifter behandlas.

Informationsägaren ska identifiera, analysera, behandla, följa upp och dokumentera risker som kan påverka Hofors kommuns informationstillgångar och de registrerades integritet negativt. Dokumentationen av detta ska vara en del av beslutsunderlaget inför förändringar.

Informationsägaren ansvarar bland annat för att:

- Informationsklassning genomförs och uppdateras löpande
- Fastställa ändamålsenliga skyddsåtgärder
- Samtliga informationstillgångar som utgör en personuppgiftsbehandling hanteras utifrån principerna och andra bestämmelser i dataskyddsförordningen
- Upprättning samt revidering görs, gällande:
    - Informationshanteringsplan
    - Registerförteckning över personuppgiftsbehandlingar
    - Förteckning över aktuell kamerabevakning
- Tröskelanalys genomförs för samtliga personuppgiftsbehandlingar
- Kontinuerligt genomföra och omvärdera riskanalyser och konsekvensbedömningar samt vidta åtgärder utifrån förändrade risker, särskilt gällande så kallade högriskbehandlingar för registrerades fri och rättigheter
- Endast behöriga får tillgång till de informationstillgångar/personuppgifter som behövs för respektive arbetsuppgift
- Vid behov ta fram egna instruktioner som behövs i verksamheten/på enheten

Information om och hantering av registrerades rättigheter
Information om vilka rättigheter den registrerade har och på vilket sätt deras personuppgifter hanteras ska i huvudsak lämnas via intranätet, för anställda, och på den offentliga webbplatsen (hofors.se) till medborgare. Den mest grundläggande informationen ska lämnas direkt när den registrerade är i kontakt med kommunen. Informationsägaren ansvarar för att de registrerade får information gällande de behandlingar som denne ansvarar för. Respektive chef ansvarar för att begäranden av registrerades rättigheter utifrån dataskyddsförordningen hanteras korrekt och effektivt inom den egna verksamheten/enheten.

Hantering av artificiell intelligens (AI)
Kommunens utforskande av AI ska ske med respekt för de svårigheter som finns relaterat till informationssäkerhet och dataskydd. Information som innehåller personuppgifter eller andra uppgifter som kan påverka kommunens informationssäkerhet ska inte användas i AI-tjänster.

AI ska inte införas i verksamheten om inte informationssäkerhets-, dataskydds- och sekretessfrågorna beaktats och hanterats. Vid införande av AI ska det säkerställas att kommunen förblir transparent och har full kontroll samt ägandeskap över informationen. Det ska tydligt framgå om information, beslut eller annat material är framtaget med hjälp av AI. I de fall generativ AI har använts ska svar vara kontrollerade för att säkerställa korrekta fakta och referenser. Det åligger varje medarbetare att användandet av AI sker i enlighet med kommunens styrdokument.

Utbildning och avslut av anställning

Alla förtroendevalda och medarbetare ska göras medvetna om sina skyldigheter vid hantering av Hofors kommuns information samt om gällande regler för informationssäkerhet, dataskydd och sekretess.

Närmaste chef ansvarar för att medarbetaren:

- Får utbildning i informationssäkerhet och dataskydd utifrån vad som är relevant för dennes uppdrag/arbetsuppgifter
- Bibehåller en lämplig kunskapsnivå under hela uppdrags - eller anställningstiden
- Känner till gällande styrdokument för informationssäkerhet och dataskydd
- Vid avslut av uppdrag eller anställning
    - Återlämnar informationstillgångar
    - Behörighet till informationstillgångar upphävs
    - Skriftligen informeras om när fortsatt tystnadsplikt gäller

Disciplinära åtgärder kan komma att vidtas när en chef eller medarbetare brutit mot gällande styrdokument för informationssäkerhet och dataskydd.

Upphandling, kravspecifikation och uppföljning av externa parter

Upphandling och införande av IT-system

Informationsägaren ansvarar för att informationssäkerhet och dataskyddsarbetet är integrerat i upphandlings- och avtalsuppföljningsprocessen. Infosäk och dataskydd ska vara en del av grundparametrarna när kravställningar för system och funktionalitet tas fram inklusive principerna om inbyggt dataskydd och dataskydd som standard.

Innan upphandling av IT-system, så väl i egen drift som molntjänster ska informationsklassning genomföras. Resultatet av den utgör underlag till teknisk kravställning samt avgör om en konsekvensbedömning för informationsbehandlingen behöver göras, vilket även den i förekommande fall utgör underlag till teknisk kravställning.

Övergång från egen drift till molndrift, utan att byta system, kan likställas med ett nytt införande och samma tillvägagångsätt som vid en upphandling ska tillämpas. Kommunens IT-organisation ska alltid involveras vid upphandling av IT-system samt vid övergång från egen drift till molndrift.

Inga system eller molntjänster som innebär att personuppgifter överförs till tredjeland eller till land som enligt EU-kommissionen inte uppnår adekvat skyddsnivå ska införas. Vid behov ska kompletterande effektiva skyddsåtgärder införas för att säkerställa att inga personuppgifter överförs till tredjeland.

Uppgifter som omfattas av sekretess bör inte överföras till externa molntjänster. I undantagsfall kan en riskbedömning, inbegripen sekretessprövning, avgöra om en uppgift som omfattas av

sekretess får överföras till en molntjänstleverantör som finns inom EU/EES och som inte omfattas av lagstiftning i tredjeland som kan ge utländska myndigheter åtkomst till uppgifterna.

Externa parter
Externa parter utgörs av:

- Helägda bolag
- Delägda bolag
- Kommunalförbund
- Kommungemensamma nämnder och förvaltningar
- Externa utförare
- Leverantörer
- Konsulter
- Andra som har behörighet att använda kommunens information

Externa parter med åtkomst till kommunens IT-miljö är skyldiga att följa kraven på informationssäkerhet och dataskydd i denna riktlinje.

När Hofors kommuns informationstillgångar eller personuppgifter hanteras av en extern part ska de skyddas på ett likvärdigt sätt som när kommunen hanterar informationen själv. Endast externa parter som kan garantera lämpliga tekniska och organisatoriska säkerhetsåtgärder ska anlitas.

När kommunen anlitar aktörer utanför organisationen ska personuppgiftsansvar identifieras och dokumenteras. Kraven som ställs på externa parter ska regleras och fortlöpande följas upp, särskilt vid förändringar som påverkar det som är överenskommet.

Det åligger varje enskild individ att följa gällande lagar, standarder och övrig styrning inom informationssäkerhet och dataskydd.

Nätverks- och systemsäkerhet

Driftsäkerhet
Drift av IT-miljö, system och tillhörande informationsbehandlingsresurser ska ske utifrån fastställda rutiner för gemensam infrastruktur och de specifika säkerhetskrav som ställs genom verksamhetens informationsklassning.

Interna och externa sårbarhets- och penetrationstester ska genomföras, i syfte att verifiera att säkerhetsåtgärderna har förväntad effekt. Det ska finnas processer som säkerställer att system- och driftdokumentation är aktuell. Känslig dokumentation ska endast vara tillgänglig för behörig personal. Organisationen ska skyddas från förlust av data genom säkerhetskopiering.

Loggning och övervakning ska tillämpas för att upptäcka och hantera sårbarheter som kan påverka informationssäkerheten samt ge förutsättningar för att händelsekedjor kan återskapas vid misstanke om brott. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst. Övervakning innefattar bland annat:

- Scanning av skadlig kod
- Kontroll av nätverksanslutningar
- Kontinuerlig kontroll av administratörsrättigheter
- Genomlysning och rapportering av konton som inte kan associeras med en ägare eller verksamhetsprocess.

Funktioner och tjänster i driftmiljön som inte används ska avinstalleras eller avaktiveras. När IT-utrustning utrangeras, kasseras, säljs eller på annat sätt lämnar kommunen ska först avinstallation och radering av information genomföras.

Nätverk
Samtliga anslutningar till Hofors kommuns interna IT-miljö ska vara godkända och dokumenterade.

Vid kommunikation över öppna nätverk ska särskilda skyddsåtgärder vidtas för att garantera konfidentialitet och riktighet för data som överförs som exempelvis kryptering och multifaktorautentisering. Alla anslutningar till nätverk ska vara dokumenterade och godkända.

Enheter och applikationer
Privata enheter och konton får ej användas i arbetssyfte. Privata enheter och konton får inte heller anslutas/logga in till kommunens produktionsnätverk. Konton och licenser som erhållits i arbetssyfte får inte användas i privata syften, till exempel jobbmailen. Icke kommunägda enheter får ej användas i arbetssyften. Enheter köpta via annan än kommunens IT får endast användas då informationssäkerheten för Hofors kommuns information kan säkerställas. Autentiseringsmetoder omfattas inte av denna begränsning.

Enheter såsom surfplattor eller kioskdatorer för besökare, patienter, deltagare eller liknande, ska vara skilda från kommunens produktionsnätverk och får endast konfigureras på ett sådant sätt så de inte kompromissar informationssäkerhet eller dataskydd.

Endast godkända applikationer ska vara aktiverade och möjliga att använda i organisationens IT-miljö. Alla applikationer ska förvaltas av utsedd ansvarig, antingen av systemförvaltare eller annan utpekad ansvarig medarbetare. Denne ska säkerställa livscykelhanteringen och distribution av säkra versioner.

Fysisk och miljörelaterad säkerhet

Kraven på fysisk säkerhet ska tillämpas för alla lokaler där information hanteras, samt för all utrustning som används för informationshantering. Information och utrustning ska skyddas på ett likvärdigt sätt oavsett om den hanteras innanför eller utanför organisationens lokaler. Ansvaret för detta utgår från den verksamhet som nyttjar lokalerna eller utrustningen, bland annat genom att ställa krav på säkerhetsåtgärder gentemot fastighetsägare, leverantörer etcetera.

Utrymmen som innehåller informationstillgångar ska skyddas genom åtgärder som säkerställer att endast behöriga får tillträde till tillgångarna.

Utrustning som innehåller lagringsmedier bör granskas för att säkerställa att all känslig information och licensierade program har avlägsnats eller överskrivits på ett säkert sätt före avveckling eller före återanvändning.

Incidenthantering

Informationsägaren ska säkerställa att informationssäkerhets- och personuppgiftsincidenter rapporteras, dokumenteras och följs upp inom respektive nämnd. Insamling och bevarande av underlaget ska hanteras på ett effektivt sätt med tanke på eventuella disciplinära och rättsliga åtgärder. Informationsägaren fattar beslut om lämpliga åtgärder som kan behöva genomföras för att mildra incidentens effekter. Vid behov ska en åtgärdsplan upprättas. Lärdomar ska dras av inträffade incidenter för att stärka och förbättra säkerhetsåtgärderna.

Vid inträffande av en personuppgiftsincident som utgör hög risk för registrerades rättigheter ska informationsägaren informera om incidenten på lämpligt sätt, beroende på incidentens karaktär och omfattning.

Incidenter som är av allvarligare karaktär ska rapporteras till säkerhetschefen. Incidenter där brott eller misstanke om brott föreligger ska alltid polisanmälas.